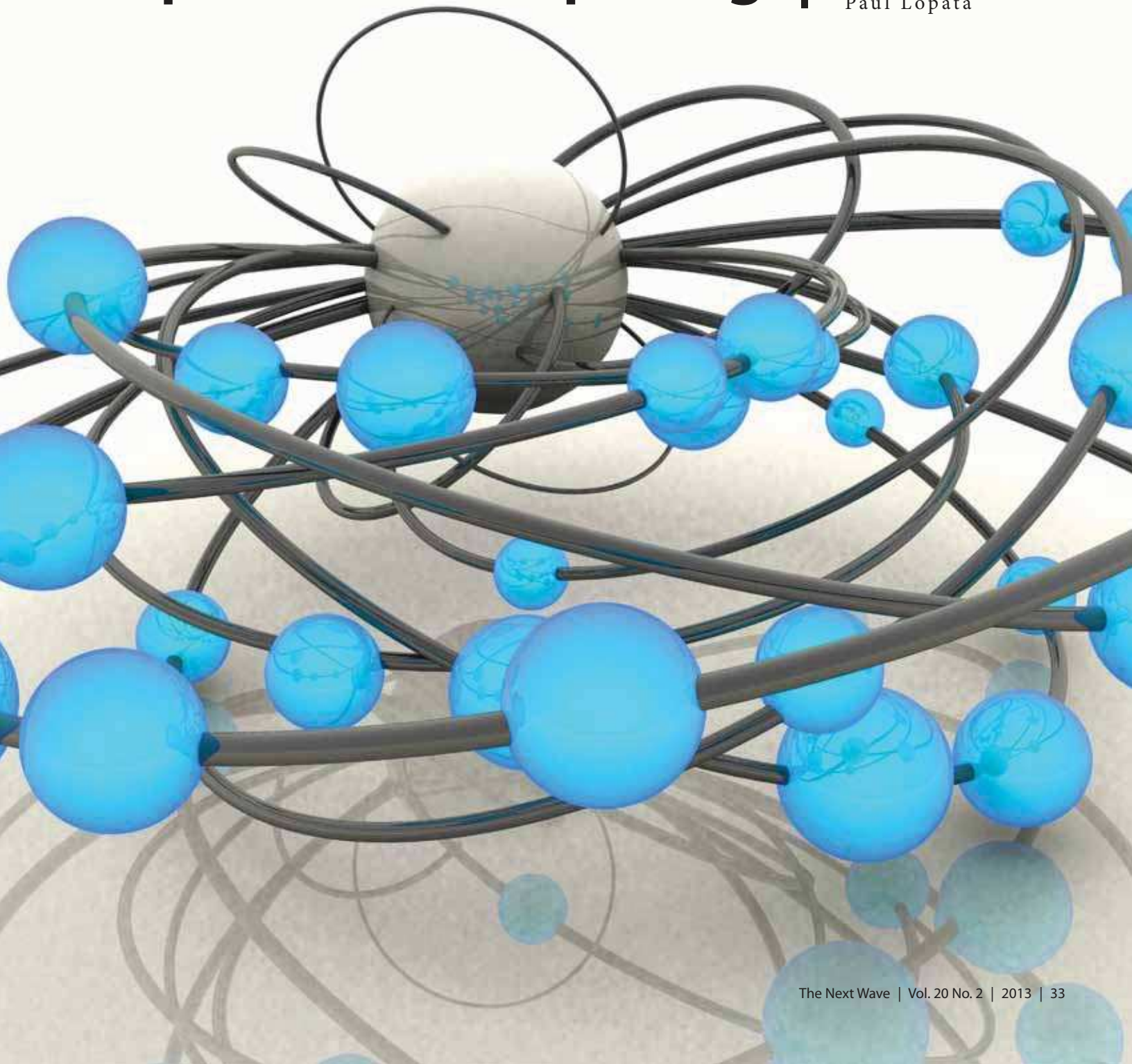


Beyond digital

A brief introduction to quantum computing |

Paul Lopata



Introduction

Computers are based on logic. These fundamental rules of logic dictate the types of problems that can be solved on a computing machine. These rules of logic also determine the resources required to complete a calculation. From the early years of computing machines to the present, the most successful computer designs have utilized two-level digital logic. The amazing success of modern-day computing technology is based on the algorithmic strengths of digital logic paired with the stunning technological advances of silicon complementary metal-oxide semiconductor (CMOS) chip technology. Processor chips and memory chips built out of silicon CMOS technology have provided a continually improving platform on which to perform digital logic.

Despite the well-known successes of computing machines based on digital logic, some algorithms continue to be difficult to perform—and some problems are intractable not only on existing machines but on any practical digital-logic machine in the foreseeable future! These intractable problems serve as both a curse and a blessing: A curse because solutions to many of these intractable problems have significant scientific and practical interest. A blessing because the computational difficulty of these intractable problems can serve as a safeguard for secure data storage and secure data transmission through the use of modern encryption schemes.

It is clear that the only algorithmic way to solve these intractable problems is to utilize a computing machine that is based on something other than standard digital logic.

One such path toward developing a “beyond-digital logic” machine is in the field of quantum computing. Quantum computing is still in the early stages of its development, and most of its advances are being reported from universities and basic research labs. Three major insights have led to the current understanding that quantum computing technology may have a significant potential for solving some of these algorithmically intractable problems:

1. Specific algorithms have been developed to solve mathematical problems on a (yet-to-be-developed) quantum computer that are otherwise intractable using standard digital logic;

2. Physical systems exist that can be used as the basic building blocks for a machine to implement these quantum algorithms;
3. There are ways to effectively handle errors that will inevitably occur when running an algorithm on one of these quantum computing machines.

This article introduces quantum computing through a discussion of these three insights and the technical literature that underpins this exciting and fast-moving field.

Quantum algorithm discoveries

When discussing the speed of an algorithm, it is useful to break the algorithm down to a basic set of steps, or gate operations, that can be repeated over and over again to complete the calculation. Once an algorithm has been written down in terms of a fixed-gate set, all that remains is counting up the number of gates required for a particular problem size to determine how many resources are required to finish the calculation. When a problem is said to be intractable, it is because the number of gates required to complete the calculation is so overwhelmingly large that the algorithm will not finish in a practical amount of time.

The first quantum algorithm discovered to have a speedup over algorithms based on digital logic came from David Deutsch in the first of a series of two papers in the *Proceedings of the Royal Society of London A* (from 1985 and 1989). The algorithm Deutsch devised to demonstrate this speedup over digital logic is something of a toy problem—it involves two narrowly defined classes of functions and tries to determine whether a function falls into one or the other of these two classes. While this toy problem has extremely limited practical interest, it was very useful in demonstrating that there is potential for a quantum computer, based on its beyond-digital logic, to solve problems faster than computers based on digital logic. This algorithmic discovery, along with the quantum circuit formalism spelled out by David Deutsch, spurred on further algorithm development.

Whereas Deutsch’s algorithm had extremely limited utility beyond a first demonstration, an algorithm later developed by Peter Shor proved to be of more widespread interest. What became known as Shor’s Algorithm provides a speedup for finding the unique

prime factors of a number—a problem of historic interest that gets extremely difficult as the number to be factored gets larger and larger. Shor’s Algorithm for factoring remains one of the best-known examples of a seemingly intractable problem that is potentially solved using a quantum computer. Many other quantum algorithms have been invented, each for tackling some difficult mathematics problem. (See the further reading section for further details on the Deutsch algorithm and Shor’s Algorithm, as well as details on the many other algorithmic discoveries and their advantages.)

It must be noted that not all algorithms achieve a speedup when tackling the problem with a quantum computer. That is, a quantum computer will provide an improvement on solving *some* problems, but will not provide an improvement on solving *all* problems. As with the other aspects of quantum computing described below, quantum algorithm development remains a vigorous open field of investigation.

Physical implementations of a quantum computer

Building and operating devices to implement the beyond-digital logic of quantum computing has been the focus of intense effort since the early quantum algorithm discoveries. A great deal of progress has been made in several different technologies toward these goals, with many impressive early demonstrations. This includes demonstrating some small algorithms with a handful of logic operations.

Demonstrating the basics of beyond-digital logic requires exquisite control over the tiniest parts of a physical system. At this small scale, the behavior of these systems is described by the laws of quantum physics. By utilizing a system governed by the laws of quantum physics, beyond-digital logic becomes possible.

Exquisite control is needed to prevent the introduction of damaging noise into the system during the control process because as noise is introduced the rules of quantum physics that describe the behavior of these small systems get washed out. (This is, in some sense, why the broader world around us is seen to obey the everyday rules of classical physics rather than quantum rules that dominate the behavior of

very small systems. The jostling of the many small systems against one another contributes to the overall noise that washes out the quantum effects at a large scale.) The term *coherence time* is used in the field of quantum computing to describe how long the regular behavior of a quantum system survives before an irreversible connection to the outside world sets in and the quantum effects required for beyond-digital logic are washed out.

The first step in operating on a system capable of going beyond digital logic is to identify a suitable small subsystem that is isolated enough to have a long coherence time but, at the same time, can be fully controlled without introducing too much extra noise. These contradictory system requirements— isolation (for a long coherence time) and connection to the outside world (for full control)—make the demonstration of beyond-digital logic such a challenge. (See the further reading section for more details on additional requirements on physical systems to perform quantum logic.)

Several physical systems have been used for early demonstrations of beyond-digital quantum logic. These include the following:

- ▶ Optical and microwave operations on the electronic and motional states of ionized atoms trapped in radio-frequency electric traps,
- ▶ Microwave operations on superconducting resonator circuits,
- ▶ Microwave and direct-current operations on the spin of a single electron isolated in a semiconductor,
- ▶ Linear and nonlinear optical operations on single photons,
- ▶ Optical operations on electrons in quantum dots grown into semiconductors, and
- ▶ Nuclear magnetic resonance operations on various states of a molecular ensemble.

Each of these technologies has different setup, control, and measurement techniques. Furthermore, each technology is at a different level of development, and the outlooks for future development vary wildly between technologies. While impressive strides have been made, no technology has successfully implemented more than a handful of quantum logic

operations before succumbing to its limited coherence time. (See the further reading section for information about recent review articles in *Science Magazine* that describe several of these technologies in more detail.)

Dealing with errors in a quantum machine

Every complex machine demonstrates unexpected behavior. The challenge for an engineer designing any computing machine is to design it so that the final answer at the end of an algorithm will not be wrong, even if errors creep in along the way.


The beyond-digital logic of quantum algorithms requires the data to remain isolated from external disturbances through the course of a calculation. This requirement imposes a difficult restriction on any error protection scheme that is implemented on a quantum computing machine: How do you check for errors in a way that does not impose a disturbance on the system that is too great to allow for the beyond-digital logic to be performed?

The key insight into this problem is to couple the small subsystem being used to perform the calculation to another small subsystem that also is capable of performing beyond-digital quantum logic. These two subsystems together can be used to cleverly encode the data for the algorithm so that tests can be performed on the second subsystem to check for errors on the original subsystem. And, if done correctly, these tests on the second subsystem will not disturb the original subsystem too much. Furthermore, if an error is detected, there are ways to correct this error on the original subsystem to allow the algorithm to finish without corrupting the final result.

For this quantum error protection protocol to work: 1) the two subsystems must be encoded so that the data remains intact while encoded, and 2) a subroutine algorithm to perform on these two subsystems must be devised that will robustly correct errors on the original subsystem—even if an error occurs while running this subroutine.

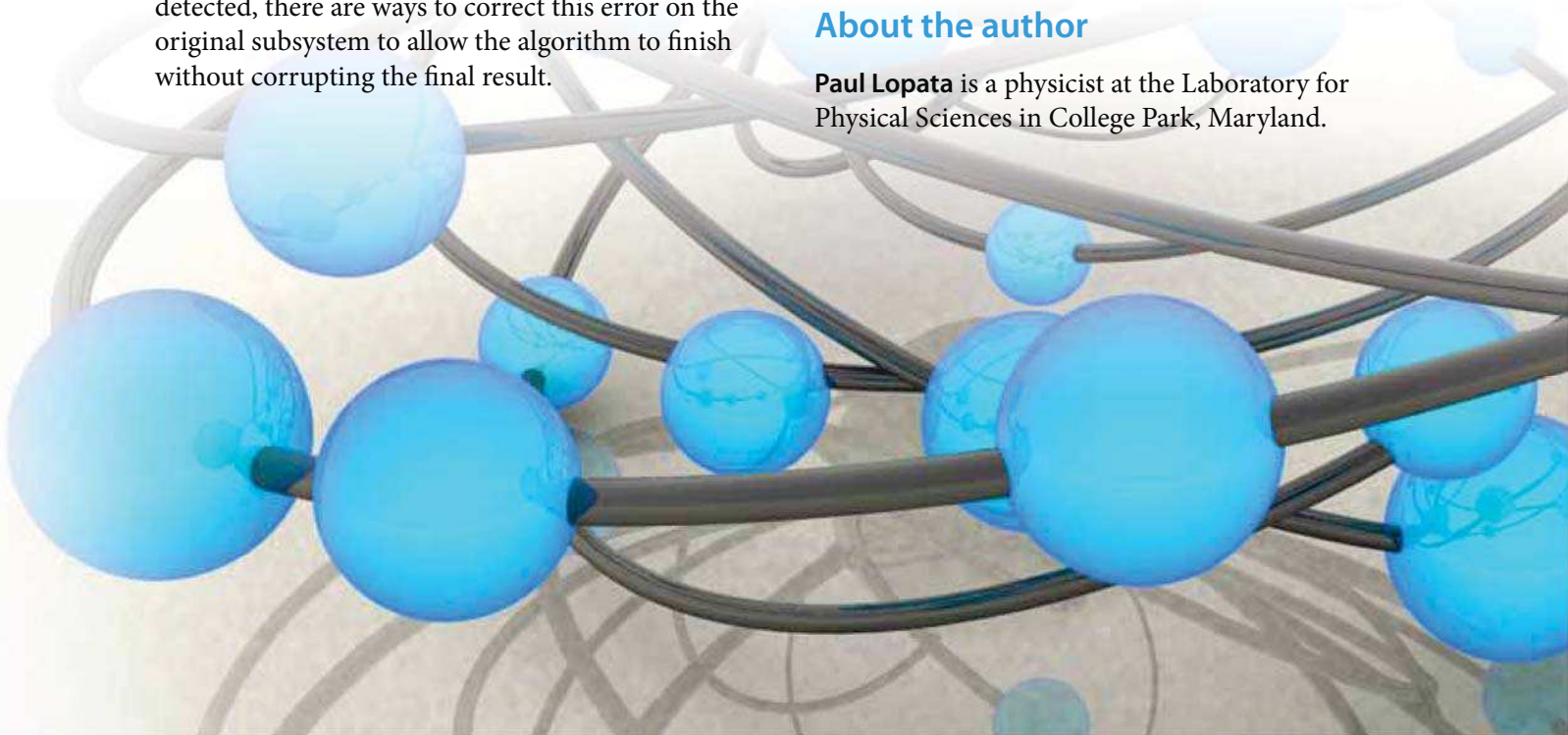
Several different schemes have been developed that accomplish these two requirements of quantum error protection, some of which are the most interesting and elegant results within the field of quantum computing. A serious challenge is the significant overhead required for encoding the data and performing these subroutines. There is also typically a very low threshold in error rates required before these schemes become effective. No experimental groups have yet demonstrated a quantum computing system of sufficient size and quality that can successfully demonstrate the full power of these quantum error protection schemes. Research continues to develop encodings that fix more errors while requiring fewer resources.

Conclusion

The rapid growth in the field of quantum computing has been a result of three key insights: discoveries of novel quantum algorithms based on beyond-digital logic, demonstration of physical systems capable of implementing beyond-digital logic, and discovery of quantum error correction. And the field of quantum computing based on its beyond-digital logic remains a fast-moving and exciting field of study. 

About the author

Paul Lopata is a physicist at the Laboratory for Physical Sciences in College Park, Maryland.



Further reading

Introduction to quantum computing

- ▶ Nielsen MA, Chuang IL. *Quantum Computation and Quantum Information*. Cambridge (UK): Cambridge University Press; 2000. ISBN-13: 978-0521635035.

This is a comprehensive and classic reference in quantum computing. It includes an introduction to the mathematics involved, algorithms, error correction, and other topics in quantum information theory. Chapter 7 on physical realizations is out of date, but the book clearly lays out the physical requirements needed for operating beyond-digital logic on a physical system.

- ▶ Mermin ND. *Quantum Computer Science*. New York: Cambridge University Press; 2007. ISBN-13: 978-0521876582.

This is a readable, high-quality introduction and reference. It is not as comprehensive as Nielsen and Chuang, but the choice of topics is well considered.

- ▶ Kitaev AY, Shen AH, Vyalı MN. *Classical and Quantum Computation*. Providence (RI): American Mathematical Society; 2002.

This is another nice introduction to major results in the field of quantum computing. More mathematical sophistication is expected from the reader.

Algorithmic developments

- ▶ All three books in the Introduction to quantum computing section of this list contain introductions to quantum algorithms.
- ▶ Jordan S. Quantum Algorithm Zoo [updated 2013 May 23]. Available at: <http://math.nist.gov/quantum/zoo/>.

Stephen Jordan at the National Institute of Standards and Technology maintains a comprehensive online catalog of quantum algorithms. This useful resource includes original references along with descriptions of the algorithms.

Experimental progress

- ▶ Special feature: Quantum information processing. *Science Magazine*. 2013;339(6124):1163–84.

This recent special section in *Science Magazine* covers several technologies in the field of experimental quantum computing. It includes review articles on ion traps, superconducting circuits, spins in semiconductors, and topological quantum computation. All of the articles are written by leaders in their respective subfield and include brief insights into the history, current state of art, and outlook on future developments.

Quantum error correction

- ▶ All three books in the Introduction to quantum computing section of this list contain introductions to quantum error correction.
- ▶ Gaitan F. *Quantum Error Correction and Fault Tolerant Quantum Computing*. Boca Raton (FL): CRC Press; 2008. ISBN: 978-0-8493-7199-8.

This book provides a comprehensive discussion of many of the major results in the field, with a focus on stabilizer codes and their fault tolerant operation.